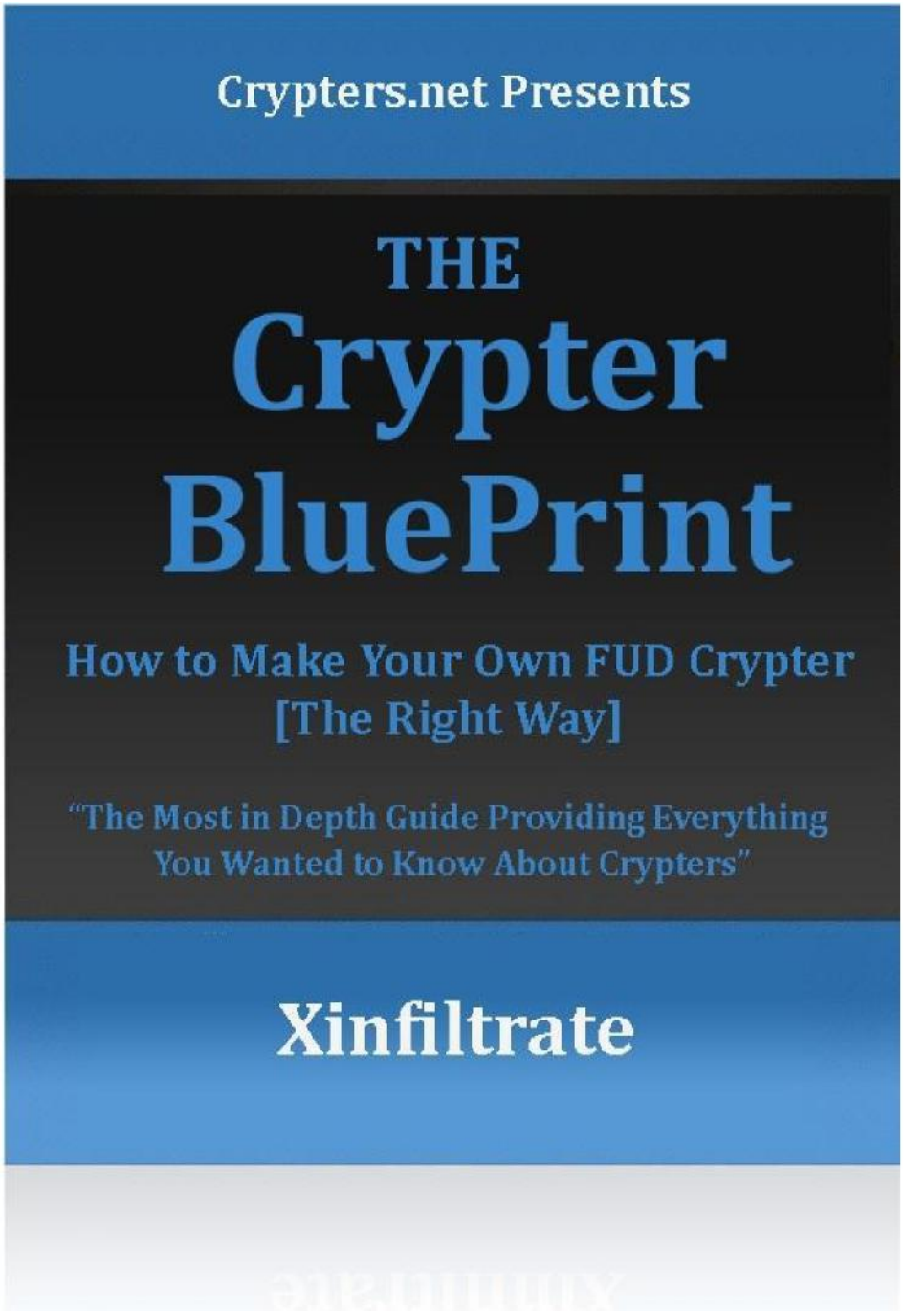


The Crypter BluePrint

The Most in Depth Blueprint on Crypters

How to Create Your own FUD Crypter [The Right Way]

...In Less Than a Week

Brought to you by,
http://crypters.net

Version 1.00
July, 2010

Limits of Liability & Disclaimer of Warranty
I AM NOT AN ATTORNEY.
DO NOT USE THE FOLLOWING TEXT UNLESS YOU HAVE YOUR OWN ATTORNEY REVIEW IT FIRST.

The author and publisher of this eBooks and the associated materials have used their best efforts in preparing this material. The author and publisher make no representations or warranties with respect to the accuracy, applicability, fitness, or completeness of the contents of this material. They disclaim any warranties expressed or implied, merchantability, or fitness for any particular purpose. The author and publisher shall in no event be held liable for any loss or other damages, including but not limited to special, incidental, consequential, or other damages. If you have any doubts about anything, the advice of a competent professional should be sought.

This material contains elements protected under International and Federal Copyright laws and treaties. Any unauthorized reprint or use of this material is prohibited.

About the Author

Little bit about me: My name is Shawn and I have been working with crypters for years. I am also the owner of http://crypters.net and http://cypherxorg.

It is rare to find quality information about crypters on the web that's why my goal with this ebook is to finally provide quality information about crypters all in one place.

Feel free to contact me by emailing: support@cypherx.zendesk.com

Table of Contents (roughly accurate)

Introduction

First I just want to give major credits to all the links to threads used in this eBooks. Massive credits to all the forum members that made them, thank you.

What you can expect from this?

I would just like to mention that if you even have the slightest interest in Crypters and making your own, you are in the right place. You will be provided with the most informative, in depth blueprint on Crypters ever put into one package before.

I am going to be real and remind you to be aware of what's required from you to get the most out of this eBooks. There is no magic buttons.. no magic pills.. Especially when programming, you have to put effort and take action on what you learn in order to succeed.

What's covered in this ebook?

This eBooks will consist of all the aspects that will get you on a flawless track for creating your own FUD Crypter or anything FUD to be honest.., this way you will gain a huge advantage. I will be giving my 100% into this eBooks so all I ask from you is to never be discouraged from the looks of anything and put your 100%.

The layout of this eBooks is constructed as follows,

The first half is pretty much aimed toward the beginner level to intermediate
And the second half is aimed toward the intermediate to advanced.

just to remind you to not exaggerate and be unrealistic, I will be teaching you all of what you need to know about Crypters and hopefully making your own.

So let's get started.

Chapter 1 – *A Crypter's* ***Core Fundamentals***

A Crypter encrypts and packs other software in a way that makes the actual bytes unreadable. People use a crypter to protect software from reverse engineering, piracy / theft, hacking / tampering. Antivirus positives can be defeated this way as well, though unfortunately this technique of using crypters is also used by hackers to make a virus and other malware undetected by antivirus software.

What's the difference between Crypter and a Packer?

A Crypter Encrypts your files and a Packer packs your files usually with the intention of making it smaller in size and sometimes for scantime undetection.

Both can look exactly the same.

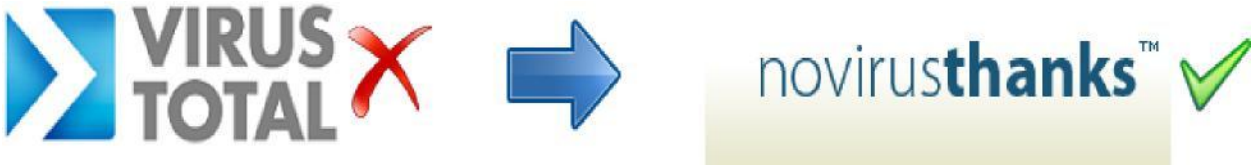
A **Runtime Crypter** encrypts the specified file and when executed (ran), it is decrypted in memory. This way antiviruses aren't able to analyze the file before executed and after executed.

A **Scantime Crypter** encrypts the specified file so antiviruses aren't able to analyze the file only before executed but NOT when execute

How do I know which antiviruses detect my file?

There are many sites with this same purpose of scanning files and giving a report of which antiviruses detect your files. The main issue leading to crypters becoming detected is because if you or someone who is in possession of your crypted file, scans it on some of these scanner sites, the crypted file will be distributed to the antivirus vendors, thus causing the crypted code overwritten on your file to become detected, which in turn causes your crypter to turn out detected.

It is recommended to scan all files you crypt on http://scanner.novirusthanks.org – while making sure the "do not distribute sample" checkbox is checked!

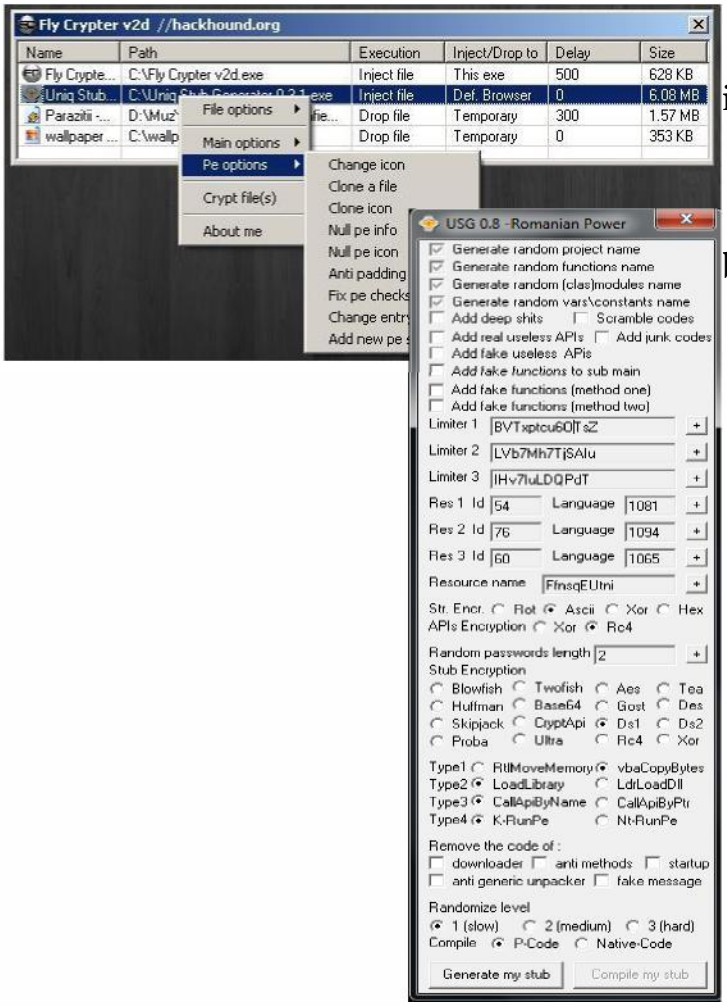


What is EOF and what is it used for?

EOF stands for End Of File. Some files like Bifrost, Medusa, and Cybergate require the end of file data in order to run without corruption, So If Crypters Don't Preserve this end of file data, your

What is a USG?

A USG is part of a crypter that generates a unique version of the stub (stub is part of crypter used to encrypt and decrypt the specified file). The purpose of this is because FUD crypters don't last forever, eventually crypters become detected over a period of time. You will understand this better later on in the eBooks. (The USG is to the right and above it is the Crypter)(But this is probably one of the most advanced USG's you will find, some can be very simple)



What is a File Binder?

A File Binder is pretty self explanatory.. It “binds” or puts to files together as one so as a result when someone opens this one file, 2 files will execute. You would usually use a file binder when being even more stealth then just simply a crypted file.

The biggest question people have when first learning what a binder is and what it does is, can you bind a .exe with something different? Like a .jpg for example? The answer is Yes, BUT.. The output of both binded files will be shown as .exe, so in a way it can defeat the purpose.

What are “anti’s” on Crypters?

Anti’s are an extra feature that comes with some Crypters. For example anti-vm, anti-debugger, anti-avira...etc these refer to bypassing or preventing something specified, so anti-debugger meaning it will prevent it from being debugged.

What is a file pumper?

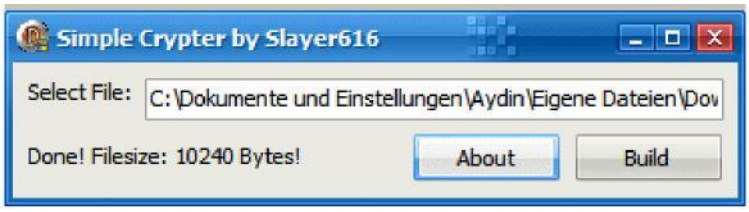
A File Pumper will “pump” your file - referring to adding more bytes to it making your file larger. The benefit of this is usually not so great but it can be ok to have and may lose a detection or 2.

Types and forms of Crypters

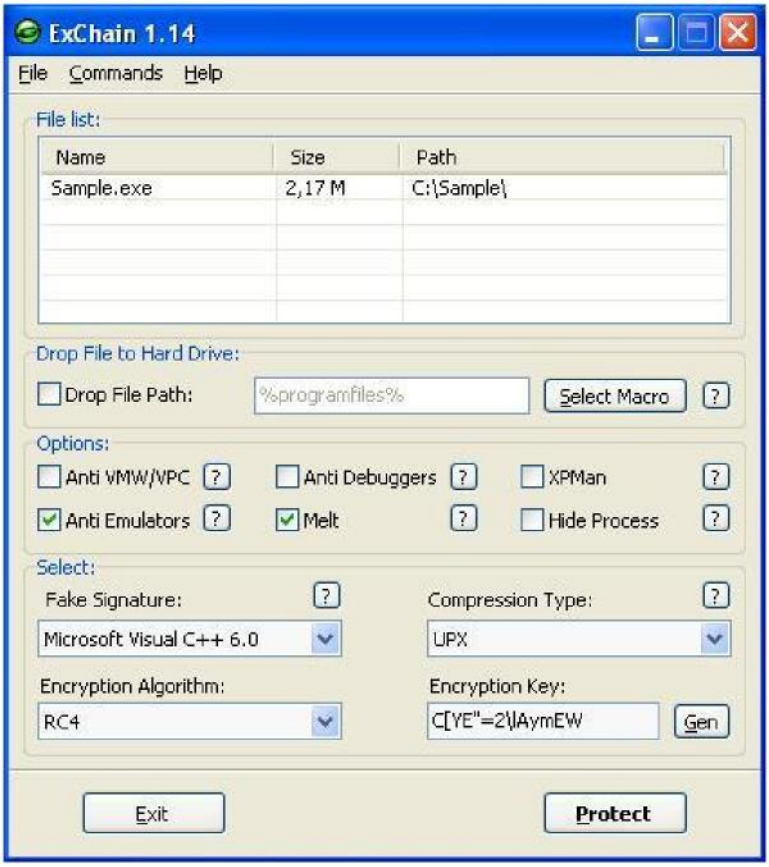
Crypters can range in many types and forms and it is important to understand these types and forms because it will help you choose a crypter more suitable for you.

Here are some simple and advanced crypters to give you a good idea, or picture in your head.

Simple GUI (graphical interface) Crypters



Here's to give you an idea of some Advanced GUI Crypters



Chapter 2 - *The most important factors you should know*

Before considering obtaining an FUD crypter of any kind, there is one thing you should know, if you don't already. It is common knowledge that all "public" (free) crypters on the web are either of the following:

- Detected (not FUD) or will become detected typically in no longer then a matter of days.
- Fake
- Dangerously packed with viruses and trojans!

It is even difficult to find a crypter with which you can purchase that will stay undetected (FUD) because the majority of all other crypters are typically being sold by hackers, these crypters are:

- Unreliable in various ways including lack of code protection and integrity.
- Not suitable for professional use cases
- Only updated to stay undetectable for a temporary period of time.
- Etc.

That is why if you are interested in obtaining an FUD crypter,

You must either create your own which is highly unlikely. This will take even more time depending on your programming knowledge. It is a very difficult and long learning process to properly mitigate antivirus software and to manage against constant antivirus updates.

Or purchase one that is professionally managed and suits your needs. (Continue reading)

Are You In Need Of A Crypter For Personal Or Professional Use?

If you are in need of a crypter for personal uses, this is the perfect choice and is widely popular: http://cypherx.org

If you are in need of a crypter for professional uses such as remotely monitoring employees and penetration testing, you need a more reliable and suitable solution, get more details here: Click Here

The Antivirus vs. Crypter Concept

Have you ever wondered how all the viruses, rats, etc, become detected by antiviruses?

Antiviruses can be much more complex than you would imagine, so learning the ways they are notified of malicious files and how they detect are essential for bypassing them.

There are 2 ways antiviruses are notified of malicious files and eventually flag your file as detected,

1. The first is

From online file scanner sites where people upload files they think might be suspicious looking, and want to know if it's actually a virus or not. They upload their files to one of these sites to check which antiviruses detect it and flag it as a virus. Once the files are uploaded, based on certain elements they are then distributed to the antivirus vendor's labs. On some online scanners there is an option available for you to check for 'no sample distribution'. Though I am not certain if this actually does what we all think. I have heard that when referencing to the websites terms of service and/or privacy policies, they will still distribute. Even though this may be true or false, it is still always a good idea to scan on sites like scan4you.net just to be safe.

Here are some antivirus scanner

websites which may distribute samples:

http://scanner.novirusthanks.org

http://virustotal.org

www.virustotal.com/

And there are also individual antivirus scanners, for

example: http://www.kaspersky.com/scanforvirus

http://www.bitdefender.com/scanner/online/free.html

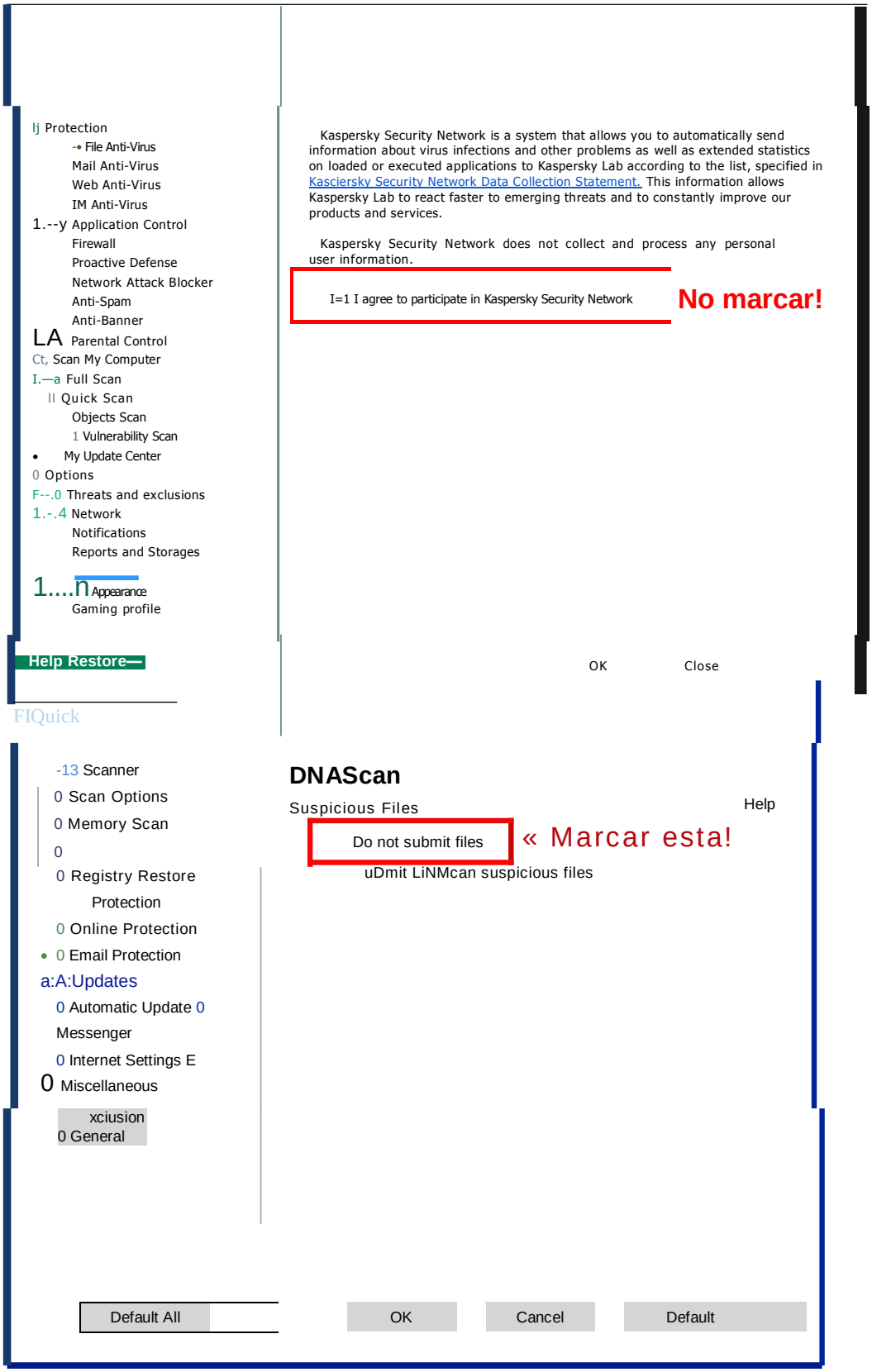
2. The Second factor is

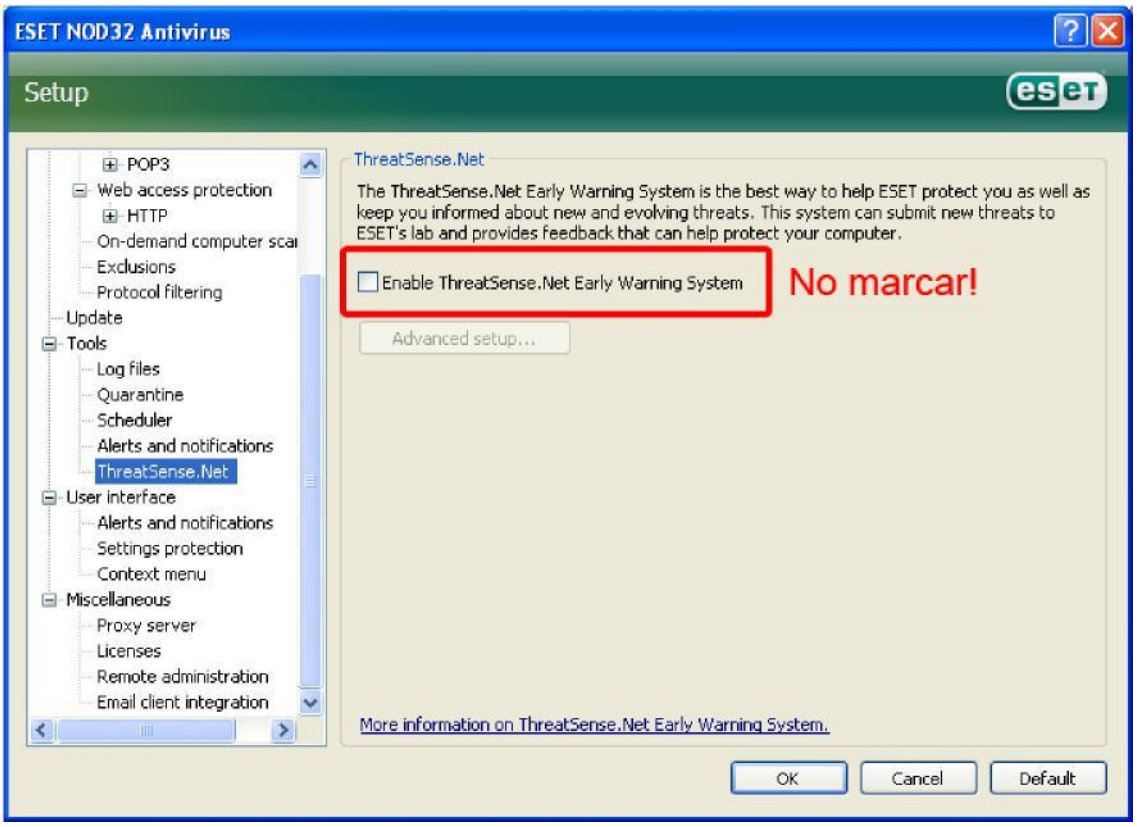
The second factor that causes antivirus detection is from the antiviruses themselves. This factor is often overlooked. This is essential information that everyone must know when using or making Crypters. Most of the time, the antivirus will automatically send detected files to their labs when any certain file becomes detected. Antivirus also owners have the option to send off a file to the vendor with a click of a button through their desktop antivirus.

What can you do about this?

well you can change the settings on your antivirus. The setting usually comes in slightly different forms, sometimes you are also asked during setup, and sometimes you just have to go into the settings or options manually, for

example:





All of what you just read is essential to keep in mind when making an FUD Crypter. The sole reason behind why public Crypters always become detected ..and usually fast, is because the majority of people do not know the antivirus vs. Crypter concept.. therefore they either blindly upload there crypted files to one of the scanner sites that distribute

also.. the antiviruses themselves are uploading there crypted files without them even noticing. Even people who make their own Crypters aren't aware of this which is why they are always wondering why there crypted files always become detected so fast.

Chapter 3 - Vb6 and Crypters

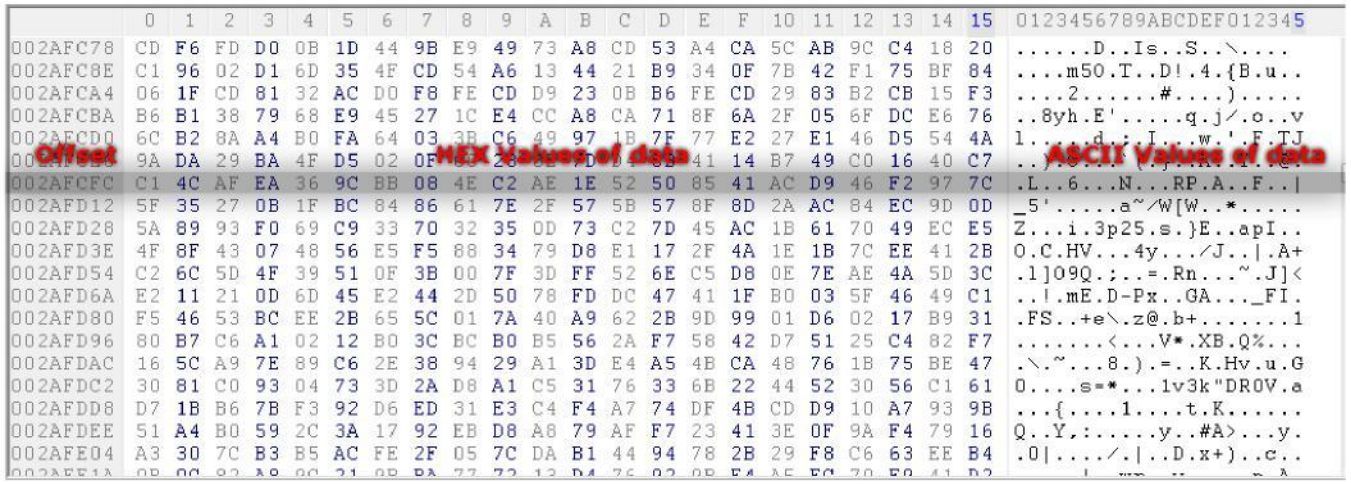
Now we are going to dive into how Crypters work, and.. how they are MADE. You will be shown the actual steps of the exact code used to create Your own Crypter.

I found these pics and info on HF somewhere ..so credits to that dude.. And if it seems a little too complicated, don't worry, as long as you get the basic idea.

What do anti-viruses look for in a file?

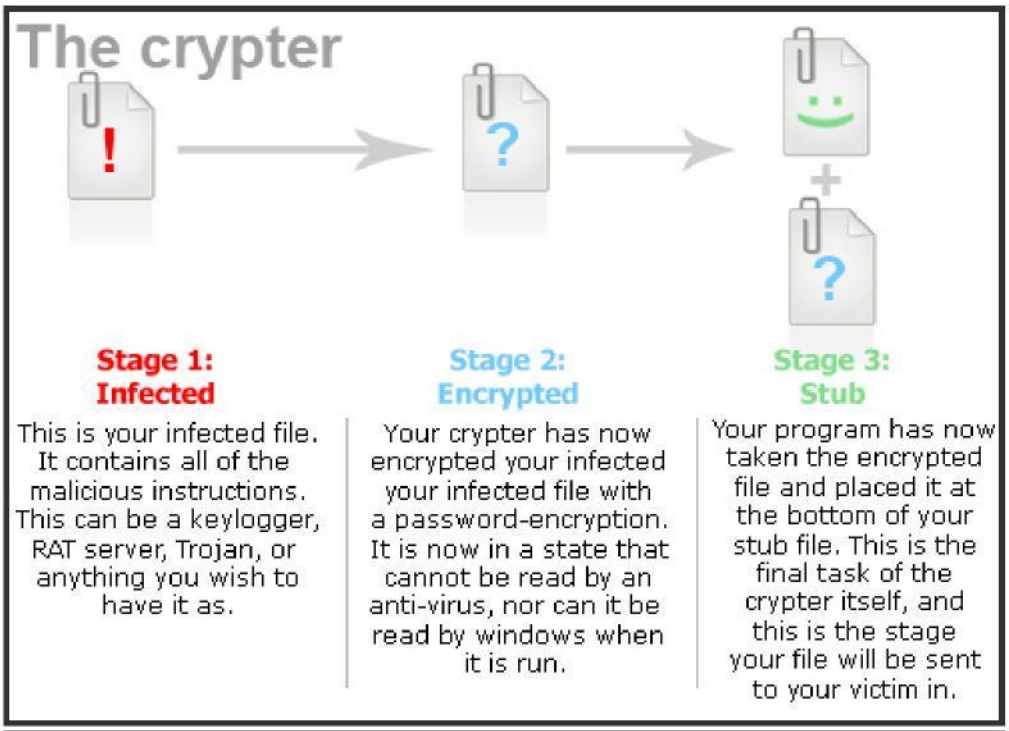
First off, you will need some basic understanding of how anti-viruses actually work.
Exe files are simply lines of instruction, and each line is called an offset.

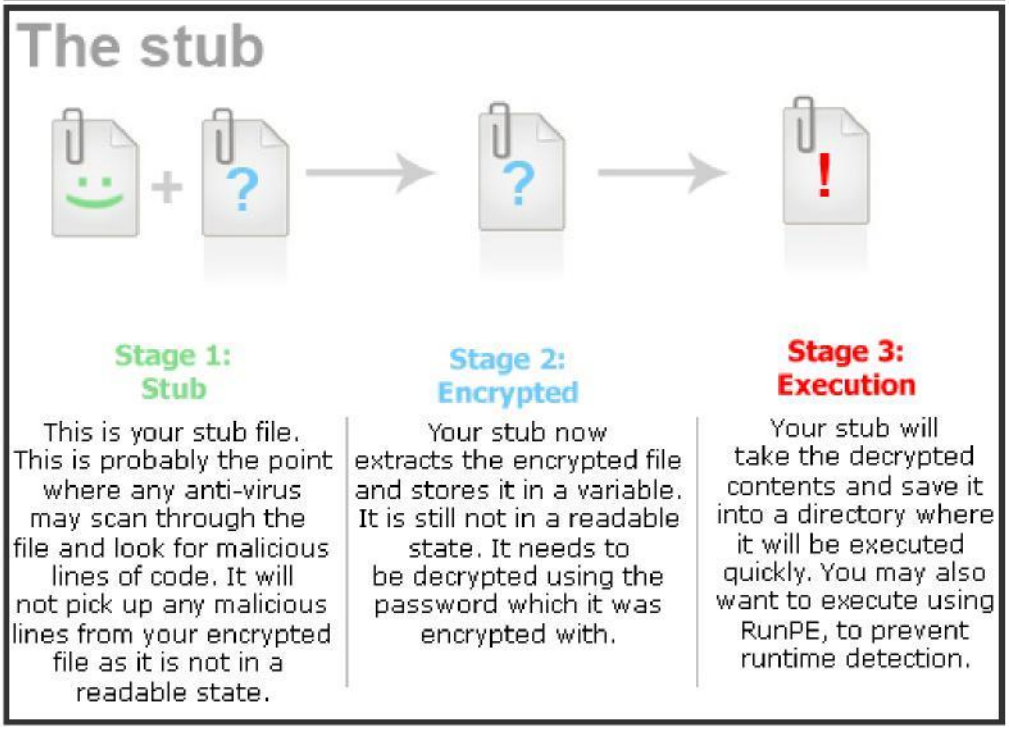
(This is a screenshot of Hex Workshop)



Anti-virus's have databases of these lines that are known to be associated with malicious files. They use that database to check against your file to see if it matches. If it does, then it is marked as infected. They do use other methods of detection, but this is the one you will learn how to avoid.

What will the program need to do?





Your crypter is going to take the contents of an infected file, encrypt them, and place it at the bottom of a seemingly virus-free file called your “stub”. Your stub file will then extracts the encrypted data from itself, decrypt it, then extract and run it. So just imagine if this stub file that is joined together with the cryped infected file is detected? well.. then all the files you crypt will also show up as detected since this stub is used with all the crypted files. This may sound like a complicated and confusing process, but it isn’t and I will explain more about it later on

Here’s another pic I found, (credits to hack hound) this explains all this in a slightly different way, maybe you will understand it better:

File crypter architecture explained.

File binding

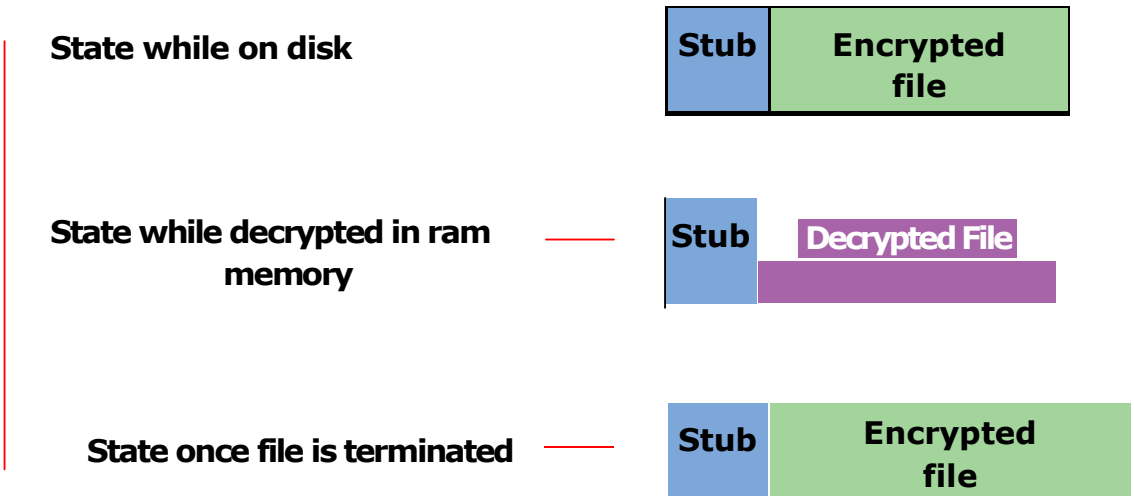
file encrypting has been around for a long time, The concept of encrypting a file "crypting", in order to make the crypted file undetectable to antivirus software or to make unpacking the file harder. In this article I will attempt to example the hows,whys and what s of file crypting.

The model of a memory executing crypter stub

The Stub

The stub is the core of the program. It is the stub's mission to carry out file decryption in memory and file execution or other custom options a programmer has given the crypter. programmers often spent a lot of time trying to reduce the size of the stub in order to reduce the file size of the outputted file (stub + encrypted file). This could also help the presenece of the stub go unnoticed if their is only a few bytes diffence from the original inputted file and the outputted file. (inputted file - outputted file) = stub size. This trend has stuck and it is now common practise to try to make the stub as small as possible. There is a myth that some people tend to fall into the trap the the smaller the size of a programmers stub the better the programmer, but this is not always the case. A stub should be judged on functionality as well as Stability and security.

Once executed



You have just reached the end of this free version of The Crypter BluePrint guide.

The next chapters include:

- *Vb6 fundamentals*
- *basic vb6 outline for creating a crypter*
- ***vb6 Crypter techniques blueprint***
- *vb6 what to do and what not to do*
- ***The Antivirus Signatures Concept***
- *Finding and pinpointing What's causing detection*
- ***The Universal Undetection Process***
- *tools and automation*
- ***What you will learn from Undetecting Crypters***
- *keeping your Crypters undetected*

To read the rest of the guide, you can purchase it at http://crypters.net/crypter-blueprint/

Or get yourself a copy of the #1 Crypter, used in over 50 countries worldwide: http://cypherx.org